FPKIPA
Federal Public Key Infrastructure Policy Authority

FEDERAL PKI POLICY AUTHORITY

June 12, 2012 MEETING MINUTES

USPS Headquarters
475 L'Enfant Plaza, SW
Conference Room: 4841
Washington, DC
9:30 a.m. – 12:00 a.m. EST

9:30	**Welcome, Opening Remarks & Introductions**	**Deb Gallagher, Chair**
9:35	**Discuss / Vote on May 2012 FPKIPA Minutes**	**Matt King**
9:45	**Criticality of FPKI Availability**	**Toby Slusher**
10:10	**Proposed Funding Model for FPKI**	**Shon Lyublanovits**
10:40	**FPKI Management Authority (FPKIMA) Report**	**Darlene Gore**
11:00	**FPKI Certificate Policy Working Group (CPWG) Report** 1. Discussion/Vote: Timestamp Change Proposal 2. FPKI Audit 3. Dual Use Keys 4. Other Updates	**Charles Froehlich**
11:30	**SHA-1 Transition Status**	**SHA-1 Affiliates**
11:35	**VA Status Update**	**John Hancock / Eric Jurasas**
11:45	**FPKIPA Chair Update**	**Deb Gallagher**
11:55	**Other Agenda Items** ○ *ICAM Update* ○ *If you cannot attend, please designate a proxy* ○ *Next FPKIPA meeting, July 10, 2012*	**Deb Gallagher**
12:00	**Adjourn Meeting**	**Deb Gallagher**

A. ATTENDANCE LIST

a. Voting Members

Organization	Name	T – Telephone P – In Person A – Absent
Department of Defense (DOD)	Mitchell, Debbie	T
Department of Energy (DOE)	Thomas, Michele	T
Department of Health & Human Services (HHS)	Slusher, Toby	P
Department of Homeland Security (DHS)	Miller, Tanyette (Proxy for Don Hagerling)	T
Department of Justice (DOJ)	Morrison, Scott	P
Department of State (State)	Rice, Barry	P
Department of Treasury (Treasury)	Wood, Dan	A
Drug Enforcement Administration (DEA CSOS)	Briggs, Sherrod (Proxy for Chris Jewell)	T
Government Printing Office (GPO)	Hannan, John	T
General Services Administration (GSA)	Gallagher, Deb	P
National Aeronautics & Space Administration (NASA)	Wyatt, Terry	T
Nuclear Regulatory Commission (NRC)	Sulser, David	P
Social Security Administration (SSA)	Mitchell, Eric	T
United States Postal Service (USPS)	Stepongzi, Mark	P
United States Patent & Trademark Office (USPTO)	Lindsey, Dan (Proxy given to GSA)	A
Veterans Administration (VA)	Jurasas, Eric	A

b. Observers

Organization	Name	T – Telephone P – In Person A – Absent
Safer Institute	Boley, Ken	P
FPKIMA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
FPKIMA (Contractor, Protiviti)	Cimmino, Giuseppe	P
IdenTrust	Cox, Jerry	P
DoS (Contractor, ManTech)	Froehlich, Charles	P
USPTO (Contractor)	Jain, Amit	T
FPKIMA (Contractor, Protiviti)	Jarboe, Jeff	P
FPKIPA (Contractor, Protiviti)	King, Matt	P
FPKIPA (Contractor, Protiviti)	Louden, Chris	P
FPKIPA (Contractor, Protiviti)	DiDuro, John	P
FPKIPA (Contractor, Protiviti)	Silver, Dave	T
CertiPath	Spencer, Judy	P
US Access	Windsor, Bill	P
eValid8	Dilley, Brian	T
ExoStar	Baker, George	T
Jacob & Sundstrom	Simonetti, Dave	T
Entrust	Khadilkar, Manny	P
Entrust	Schoen, Isadore	P
GSA	Arnold, Matt	P
GSA FAS	Shondrea Lyublanovits	P
GSA FAS	Gore, Darlene	P
GSA FAS	Stathas, Tammy	P
OMB	Bales, Carol	P

Organization	Name	T – Telephone P – In Person A – Absent
GSA	??, Jen	P

B. MEETING ACTIVITY

Welcome, Opening Remarks & Introductions, Deb Gallagher

The Federal Public Key Infrastructure Policy Authority (FPKIPA) met at the USPS Headquarters located at 475 L'Enfant Plaza SW, Washington, DC. Ms. Deb Gallagher, Chair, called the meeting to order at 9:33 a.m. EST. Those present, both in person and via teleconference, introduced themselves.

Discuss / Vote on May 8, 2012 FPKIPA Minutes, Matt King

There was a vote to approve the May 8, 2012 FPKIPA minutes. USPS motioned to approve; HHS seconded. The motion was approved unanimously.

Approval Vote for May 8, 2012 FPKIPA Minutes			
Voting members	Vote (USPS Motion; HHS Seconded)		
	Yes	No	Abstain or Absent
Department of Defense (DOD)	√		
Department of Energy (DOE)	√		
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ)	√		
Department of State (State)	√		
Department of the Treasury (Treasury)			Absent
Drug Enforcement Administration (DEA CSOS)	√		
Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC)			Absent for Vote
Social Security Administration (SSA)	√		

United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO)	√		
Veterans Administration (VA)			Absent

Criticality of FPKI Availability, Toby Slusher

Mr. Toby Slusher presented a briefing[1] and provided an update on the effort related to the Criticality of the FPKI. A Tiger Team was formed per the direction of the FPKIPA at their May 2012 meeting. Mr. Slusher reminded attendees of the purpose of the Tiger Team, which is to draft a formal letter of concern to be sent from the FPKIPA and a letter template for use by agencies to express their concerns about ensuring the FPKI is available and reliable. The goal is to raise awareness of the criticality of the FPKI to the appropriate levels within the government since agencies have become increasingly dependent on the FPKI and recognize that its availability is critical to achieving their agency missions.

The Tiger Team held a number of meetings since the last FPKIPA meeting. Participants shared good information and perspectives. The Tiger Team concluded that there is a broader issue that was identified: the future state of the FPKI. Mr. Slusher noted that a number of issues should be considered and addressed to prepare for the future state including:

- Risk mitigation
- Capacity planning – determining correct scalability for FPKI
- Critical infrastructure planning
- Continued awareness efforts (not just government, but to other entities)

Mr. Slusher asked the FPKIPA if they want the Tiger Team to pursue the three key areas mentioned in the briefing (criticality, impact, and target state). A lengthy discussion was held. The FPKIPA agreed on the following points.

- The letters could be sent to the ICAMSC and possibly OMB, but the primary audience should be the CIO Council and GSA Management.
- The Tiger Team should evaluate if the FPKI should be classified as a critical system under HSPD-7. In addition, if there are other systems classified as critical infrastructure that depend on the FPKI, why isn't the FPKI classified as critical?

[1] FPKIPA FPKI Criticality Tiger Team

- It may be beneficial to obtain input from user groups to show how end users depend on the FPKI to conduct business.
- The letter should also be sent to budget officials.
- It may be beneficial to launch an awareness campaign (e.g., create an FPKI brochure and other awareness and education materials).
- The FICAM Roadmap may include information on criticality of the FPKI (i.e., if you are implementing the FICAM roadmap, you are becoming totally dependent on the FPKI).
- Managers of systems don't fully understand the importance of the FPKI, which is why this must be raised to the CIO level.
- The letter must include a requested action specific to the audience to whom the letter is sent (i.e., simply raising awareness does not achieve the goal of the effort).

It was agreed that the Tiger Team would continue to meet and address the broader range of topics mentioned above. The Tiger Team will conclude its efforts and produce draft letters by the end of the summer 2012. In addition, an action plan of next steps will be developed and further work will continue in existing working groups.

ACTION ITEMS:

1. Mr. Toby Slusher will organize and continue to lead the Criticality of FPKI Tiger Team to achieve the following goals: (1) Produce draft letters by the end of the summer 2012, and (2) Develop an action plan of recommended next steps for additional work required from existing working groups.

Proposed Funding Model of FPKI, Shon Lyublanovits

Ms. Shon Lyublanovits and Ms. Darlene Gore from GSA FAS presented a briefing[2] on a proposed funding model for the FPKI. Ms. Lyublanovits explained that GSA has been funding the entire government-wide cost of the FPKI as a developmental cost through its working capital fund, but GSA now needs to transition the FPKI into a fee-for-service model.

Beginning in FY14, CIO Council members will pay a fee based on the number of required Personal Identity Verification (PIV) credentials (approximately $1.14 per PIV credential). GSA will absorb the cost of smaller agencies due to the limited number of credentials issued by the smaller agencies. Ms. Lyublanovits then presented the

[2] FPKI-DraftCostRecovery 6-12-12.pptx

proposed fees that would be collected from each agency and a list of alternatives that were considered. A lengthy discussion was held and the following points were raised:

- The numbers of PIV credentials used were based on what is reported to OMB on a quarterly basis (PIV-I cards are not included).
- Mr. Dave Sulser questioned how it could be more cost effective to collect from each agency rather than have a central fund, and suggested that this model caused the failure of the E-Authentication Initiative.
- Ms. Carol Bales pointed out that the funding model was not the issue with E-Authentication.
- Other funding models were suggested including a flat fee, a tiered system, and a surcharge on credentials issued by the MSO.
- The Industrial Fund might also be a source of funding that could be leveraged to provide the necessary funding.
- Ms. Debbie Mitchell also pointed out that the proposed model does not account for staff hours contributed to FPKI working groups, which is a significant cost for some agencies.
- Ms. Lyublanovits stated that this proposal would address the immediate funding concerns and the approach could be modified in future years. However, some participants questioned whether it would be possible to change the funding model once it was in place.
- Presenting a list of alternative funding models would be useful and the FPKIPA must refine the options before presenting them to OMB and the Budget Officer's Advisory Council (BOAC)

It was agreed Ms. Gore would set up conference calls on June 13 and 14, 2012 to discuss funding model alternatives. FPKIPA members were encouraged to participate.

ACTION ITEMS:

1. Ms. Gore will set up conference calls on June 13 and 14, 2012 to discuss FPKI funding model alternatives.

FPKI Management Authority FPKIMA) Report, Darlene Gore

Ms. Darlene Gore presented the FPKIMA report[3]. Ms. Gore explained that the FPKIMA will be releasing a survey to request feedback on services offered by the FPKIMA with a

[3] June2012 Slides for PA Meeting-final.pdf

goal of improving FPKIMA communications with Affiliates and finding out what additional services the Affiliates want.

An effort to enhance Path Quality Monitoring and Testing has commenced. This program will help automate path quality monitoring and revitalize the PDVal Testing program. The FPKIPA will serve as the Approver for the PDVal Testing Program and options for publication of results are still being considered.

The FPKIMA intends to submit a change proposal that will allow offline operation of the Common Policy CA. It was noted that a number of Commercial Vendors require Root CAs to be offline.

A number of status updates were provided and a review of recent and upcoming certificate issuances was reviewed.

Repository usage was also reviewed. It was noted that 30% of HTTP traffic was coming from a commercial organization supporting DoD (over 90,000 hits an hour). The FPKIMA contacted the system owner who reconfigured their application to improve how traffic was managed. It was noted that the FPKIMA cannot implement threshold controls, but they can monitor, identify issues, and work to develop resolutions. It was noted that FPKI Trust Infrastructure service was not impacted.

It was noted that the next FPKI Technical Working Group (TWG) meeting will be held on June 21, 2012 instead of June 19, 2012.

ACTION ITEMS: None

FPKI Certificate Policy Working Group (CPWG) Report, Charles Froehlich

Mr. Charles Froehlich presented the CPWG Report.

a. Discussion/Vote: Timestamp Change Proposal

Last year, Microsoft (MS) published a change requiring that all Root CAs that are listed in the MS Trust Store and that issue public-facing code signing certificates from within their infrastructures have access to a Time Stamp Authority (TSA). This change was to have gone into effect in October 2011, but in direct communications with MS, the FPKIMA obtained a delay until July 1, 2012. The Microsoft requirement places the responsibility for having valid access to a TSA on subordinate / cross certified CAs. It further states that, while CAs that issue code signing certificates are required to have a TSA capability, recipients of code signing certificates are not required to use them; they are only to be encouraged to do so. The MS language appears to limit this requirement to public facing signed code (i.e., purely internal signed code appears to be exempt for the time being).

Having the FCPCA Root certificate listed in the MS Trust Store fosters interoperability, especially with Non-Government Organization (NGO), commercial, and citizen entities, which is why this change to the policy is necessary.

The language developed for and included in the Change Proposal is intentionally non-specific; relieving the FCPCA from the responsibility to field a TSA, while allowing subordinate and cross certified CAs that sign code as many options as possible. There are currently no federal entities that have indicated that they are running a TSA that could be made available community-wide; although there are several commercial entities that provide such service. The FPKIMA has indicated that they will investigate both the need and the feasibility of standing up a FPKI community TSA at some future date.

It was noted that this change only impacts the Common Policy Certificate Policy. The CPWG has no plans to propose a change to the FBCA Certificate Policy related to TSAs. This FCPCA Change Proposal has been informally coordinated with, and received approval from MS as being sufficient to maintain the FCPCA in the MS Trust Store.

There was a vote to approve the TSA Change Proposal. HHS motioned to approve; NRC and USPC seconded. The TSA Change Proposal was approved with a 12/16 (75%) vote of all voting members.

Approval Vote to Approve the Common Policy TSA Change Proposal			
Voting members	**Vote (HHS Motion; NRC/USPS Seconded)**		
	Yes	**No**	**Abstain or Absent**
Department of Defense (DOD)	√		
Department of Energy (DOE)	√		
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ)	√		
Department of State (State)	√		
Department of the Treasury (Treasury)			Absent
Drug Enforcement Administration (DEA CSOS)	√		
Government Printing Office (GPO)			Absent for Vote
General Services Administration (GSA)	√		

National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC)	√		
Social Security Administration (SSA)			Absent for Vote
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO)	√		
Veterans Administration (VA)			Absent

b. FPKI Audit

The audit of the FPKI (i.e., FBCA, FCPCA, eGov) has been completed. While some deficiencies were identified and resolved, only two findings need to be noted.

The FPKIPA allowed the issuance of two SHA-1 certificates from the legacy FCPCA at SHA-1 after 12/31/2010. This action was performed in support of a transition in algorithms and to support interoperability. The following discrepancies resulted:

- The Key Size requirements in the FPKI Certification Practice Statement (CPS) states that, “All FBCA and FCPCA certificates are issued by a UniCert CA, which signs certificates and CRLs using SHA-256.“
- The CPS Approval procedures in the applicable policies state that, “The FPKI PA will not issue waivers.”

A Plan of Actions and Milestones (POA&M) has been prepared that addresses the identified gaps and non-compliant issues with the exception of the two noted, which cannot be resolved but were acceptable to the FPKIPA when the SHA-1 issue occurred. Both Mr. John Cornell and the CPWG have found this audit of FPKI CAs to be acceptable.

c. Dual Use Keys

DigiCert has raised some questions about the use of “Dual Use Keys” and has asked for clarification on certain terms in that regard, including defining the meaning of “legacy application” and the potential for conflict with FIPS 186 especially in relation to the DIRECT application.

At the last CPWG meeting, there was extended discussion on implementation of Dual Use Keys vis-à-vis FIPS 186-3 and SMIME/TLS involving NIST.

- FIPS 186-3 is current, but the FBCA CP contradicts it, although some legacy applications cannot or will not comply.

- NIST SP 800-57-3 focuses on TLS. However, TLS is only used for key transport, while other symmetric keys are used for encryption.

d. Other Updates

The CPWG will take up the issue of expanded use of EKUs in connection with all certificates (not just code signing as previously discussed) in conjunction with the FPKI TWG.

The CPWG will begin review of NIST SP 800-53 rev 4 and FPKI Security Controls Profiles, including an update to the Leveraging Audit Overlaps (FISMA, PIV (NIST SP 800-79), PKI Audits) document, and will begin review of the policy impacts regarding the conflict between RFC 3280 vs RFC 5280 and the policy impacts of the new RFC draft-ietf-pkix-caa-07.

SHA-1 Transition Status, SHA-1 Affiliates

Mr. Matt King reminded the FPKIPA that Affiliates who have not transitioned to SHA-2 should be prepared to provide updates on their transition status by the next FPKIPA meeting.

VA Status Update, John Hancock / Eric Jurasas

No update was received from VA. Ms. Judy Spencer pointed out that VA had presented a schedule showing when all the issues would be resolved. The schedule showed all the actions complete by March of 2012.

FPKI Chair Update, Deb Gallagher

Ms. Deb Gallagher presented the FPKIPA Chair Report[4]. Ms. Gallager mentioned that an internal GSA meeting will be held next week to discuss ICAM Governance. In addition, a FIPS 201 Evaluation Program Agency Day will be held on June 19, 2012. An RFP is expected in 2-3 weeks. The FCCX efforts will potentially result in a service that helps agencies adopt third-party credentials. A list of upcoming meetings is listed below.

Meeting	Date
ISIMSC	**June 25, 2012**
CPWG & TWG	**June 21, 2012**

[4] FPKIPA Chair Report_12JUN12.ppt

CPWG (replaces 1st Tuesday in July)	**June 28, 2012**
ICAMSC	**June 27, 2012**
IAB	**June 27, 2012**
Agency Day – FIPS 201 EP	**June 19, 2012**

Summaries of change proposals, cross-certifications, and FPKI Documentation were also reviewed.

Other Agenda Items, Deb Gallagher

No other agenda items were discussed.

Adjourn Meeting

The meeting was adjourned at 11:59 a.m. EST.

FPKIPA Action Items

No.	Action Statement	POC	Start Date	Target Date	Status
433	Matt King will place a deadline for C4CA responses for the first August CPWG for all agencies to provide their position on the necessity of the C4CA	Matt King	July 12, 2011	August 8 2011	Closed
434	Ms. Brown will send the MA report to the PA after changing the TWG date.	Wendy Brown	July 12, 2011	July 19, 2011	Closed
435	Ms Cheryl Jenkins will arrange an ad hoc meeting with Microsoft to address the CAPI path validation issues prior to Sept 15, 2011	Cheryl Jenkins	July 12, 2011	September 15, 2011	Closed
436	Ms. Gallagher will send an email with the request for a statement of need for removing the non-revocable certificates to the voting PA members .	Deb Gallagher	July 12, 2011	August 9, 2011	Closed
437	Mr. Matt King will send the EGTS briefing to the group	Matt King	July 12, 2011	August 9, 2011	Closed
438	Ms Gallagher will publish the Digital Signature Guidance once a final review is complete; will be published on the web as well.	Deb Gallagher	July 12, 2011	September 13, 2011	Open

No.	Action Statement	POC	Start Date	Target Date	Status
439	Ms. Wendy Brown and Mr. Matt King work to establish a fed-only email list.	Matt King / Wendy Brown	August 9, 2011	December 13, 2011	Closed
442	Mr. King will send ORC PIV-I testing documentation and E-vote to the FPKIPA mail list	Matt King	August 9, 2011	September 13, 2011	Closed
443	Mr. King will send DigiCert audit letter and E-vote to the FPKIPA mail list	Matt King	August 9, 2011	September 13, 2011	Closed
446	The Timestamp Server White Paper will be added to the CPWG and FPKIPA agendas.	FPKIMA	August 9, 2011	September 13, 2011	Closed
449	All FPKIPA members shall submit their nomination for a new FPKIPA Chair to Ms. Gallagher and Mr. King by October 31, 2011	All Voting Members	September 13, 2011	October 31, 2011	Closed
450	Ms. Mitchell will provide DoD Lessons Learned from the LDAP transition by Oct 6, 2011.	Debbie Mitchell	September 13, 2011	October 6, 2011	Closed
451	At the 25 October meeting, the CPWG will add language to the FPKIPA Charter – Option B indicating that the CIO Council will appoint the FPKIPA Chair from a list of nominees put forward by the FPKIPA membership	Matt King	October 18, 2011	October 25, 2011	Closed

No.	Action Statement	POC	Start Date	Target Date	Status
452	At the 25 October meeting, the CPWG will discuss revising the FBCA Device Change Proposal to address Mr. Cooper's concerns that language in the FBCA change proposal was unnecessary	Matt King	October 18, 2011	October 25, 2011	Closed
453	Mr. Matt King to obtain Ms. Gallagher's signature on Charter and post to idmanagemnt.gov	Matt King	Nov 8, 2011	Dec 13, 2011	Closed
454	Ms. Gallagher and Mr. King to find out what's needed to participate in CAB Forum.	Matt King, Deb Gallagher	Nov 8, 2011	Dec 13, 2011	Open
455	Mr. Hancock of VA will send the VA status briefing presented in the 8 November FPKIPA meeting to Matt King for distribution and report back with a VA mitigation plan at the next FPKIPA meeting.	Matt King, John Hancock (Va)	Nov 8, 2011	Dec 13, 2011	Closed
456	Mr. King to distribute the VA briefing summarizing actions taken as of November 8, 2011 once the briefing is received from VA.	Matt King	Nov 8, 2011	Dec 13, 2011	Closed
457	Mr. Matt King will consult Mr. John Cornell and Mr. Tim Polk to determine if the intent of the Common Policy audit requirements is to require an Audit Letter or a full Audit Report.	Matt King	Dec 13, 2011	Jan 10, 2012	Closed

No.	Action Statement	POC	Start Date	Target Date	Status
458	Mr. Matt King will evolve the document tracking table to provide detailed status for the FPKI Community (NIST documents that are in the review process should also be included).	Matt King	Dec 13, 2011	Mar 30, 2012	Closed
459	Mr. Matt King will distribute the VA Status Update to the FPKIPA Mail List when Mr. Eric Jurasas provides a copy	Matt King	Jan 10, 2012	Jan 20, 2012	Closed
460	The FPKIMA will work with Mozilla to determine what Mozilla will accept if we do not provide CPSs	Wendy Brown	May 8, 2012	Jun 30, 2012	Open
461	Mr. Toby Slusher will form a focus group to develop the letters related to the criticality of the FPKI and address the issues discussed in the 8 May 2012 FPKIPA meeting	Toby Slusher	May 8, 2012	Jun 30, 2012	Closed
462	Mr. Toby Slusher will organize and continue to lead the Criticality of FPKI Tiger Team to achieve the following goals: (1) Produce draft letters by the end of the summer 2012, and (2) Develop an action plan of recommended next steps for additional work required from existing working	Toby Slusher	June 12, 2012	August 31, 2012	Closed

No.	Action Statement	POC	Start Date	Target Date	Status
	groups.				
463	Ms. Gore will set up a conference call on June 13, 2012 to discuss FPKI funding model alternatives.	Darlene Gore	June 12, 2012	Jun 12, 2012	Closed